

# Table of Contents

## Keynote Talk

Lifting Reference Monitors from the Kernel .....	1
<i>F.B. Schneider</i>	

## Invited Talks I

Authenticity Types for Cryptographic Protocols .....	3
<i>A. Gordon</i>	
Verifying the SET Protocol: Overview .....	4
<i>L.C. Paulson</i>	

## Protocol Verification

Interacting State Machines: A Stateful Approach to Proving Security ....	15
<i>D. von Oheimb</i>	
Automatic Approximation for the Verification of Cryptographic Protocols .....	33
<i>F. Oehl, G. Cece, O. Kouchnarenko, D. Sinclair</i>	
Towards a Formal Specification of the Bellare-Rogaway Model for Protocol Analysis .....	49
<i>C. Boyd, K. Viswanathan</i>	

## Invited Talks II

Critical Critical Systems .....	62
<i>S. Stepney</i>	
Analysing Security Protocols .....	71
<i>D. Gollmann</i>	

## Analysis of Protocols

Analysis of Probabilistic Contract Signing .....	81
<i>G. Norman, V. Shmatikov</i>	
Security Analysis of (Un-) Fair Non-repudiation Protocols .....	97
<i>S. Gürgens, C. Rudolph</i>	
Modeling Adversaries in a Logic for Security Protocol Analysis .....	115
<i>J.Y. Halpern, R. Pucella</i>	

## Security Modelling and Reasonning

Secure Self-certified Code for Java . . . . .	133
<i>M. Debbabi, J. Desharnais, M. Fourati, E. Menif, F. Painchaud, N. Tawbi</i>	
Z Styles for Security Properties and Modern User Interfaces . . . . .	152
<i>A. Hall</i>	

## Invited Talks III

Cryptographic Challenges: The Past and the Future . . . . .	167
<i>B. Preneel</i>	
TAPS: The Last Few Slides . . . . .	183
<i>E. Cohen</i>	

## Intrusion Detection Systems and Liveness

Formal Specification for Fast Automatic IDS Training . . . . .	191
<i>A. Durante, R. Di Pietro, L.V. Mancini</i>	
Using CSP to Detect Insertion and Evasion Possibilities within the Intrusion Detection Area . . . . .	205
<i>G.T. Rohrmair, G. Lowe</i>	
Revisiting Liveness Properties in the Context of Secure Systems . . . . .	221
<i>F.C. Gärtner</i>	

<b>Author Index</b> . . . . .	239
-------------------------------	-----

Formal Aspects of Security

First International Conference, FASEc 2002, London,

UK, December 16-18, 2002, Revised Papers

Abdallah, A.E.; Ryan, P.; Schneider, S. (Eds.)

2003, X, 246 p., Softcover

ISBN: 978-3-540-20693-4